REMARKS/ARGUMENTS

The Office Action mailed June 27, 2005 has been reviewed and carefully considered. Claims 1-2, 4-6, and 13 have been amended. Claims 1-17 are pending in this application, with claims 1 and 13 being the only independent claims. Reconsideration of the above-identified application, as herein amended and in view of the following remarks, is respectfully requested.

In the Office Action mailed on June 27, 2005, claims 1-17 stand rejected under 35 U.S.C. §102(e) as anticipated by U.S. Patent No. 6,105,134 (Pinder).

Claims 13-17 stand rejected under 35 U.S.C. §102(e) as anticipated by U.S. Patent No. 6,105,013 (Curry).

The present invention relates to a method of implementing a digital signature. From the material to be signed, a first hash code in computed (see page 11, lines 4-5 of the present application). The hash code is added to the material to be transferred to the mobile station (page 4, lines 26-28; page 11, lines 11-14; Figs. 1-3). After being transferred to the mobile station, the material is signed using the mobile station (page 4, lines 28-30; page 11, lines 18-20). The signed material and hash code is transferred from the mobile station to a payment machine or a bank (Fig. 1 and Fig. 2) where the signed material is verified for authenticity.

The claims have been amended to place them in better form. For example, independent claim 1 is amended such that each method step begins with the gerund form of a verb. No new limitations are added. Independent claim 1 recites "digitally signing, using the mobile station, the material and first hash code transferred to the mobile station", and "verifying the authenticity of the signed and transferred material by comparing the signed hash code with the first hash code computed from the material before signature". Independent claim 13 includes similar

limitations of "the mobile station comprises signing means for the signing of the material transferred into it" and "the payment machine comprises means for verifying the authenticity of the signed and transferred material by comparing the signed hash code with the first hash code computed from the material before signature".

Pinder fails to disclose, teach or suggest these limitations because Pinder only discloses a one-way transfer. Pinder discloses a cable television system in which programs are broadcast to set-top units which selectively decrypt the programs for display. Pinder discloses that the sender generates a hash code and that the receiver uses the same hash function on the received material to generate the same hash code (e.g., see col. 8, lines 16-28, and 45-47 of Pinder). Since Pinder discloses that the receiver merely receives the message and separately generates its own hash code based on the received material, Pinder fails to teach or suggest the step of signing the material or signing the hash code at a mobile station, as is expressly recited in independent claims 1 and 13. Furthermore, since Pinder relates to a one-way transmission of material, Pinder fails to teach or suggest "verifying the authenticity of the signed and transferred material by comparing the signed hash code with the first hash code computed from the material before signature", as recited in claims 1 and 13. Accordingly, independent claims 1 and 13 are not anticipated by and are also allowable over Pinder.

Independent claim 13 is also rejected as anticipated by Curry. However, Curry fails to teach or suggest a payment machine that comprises means for computing a first hash code from the material to be signed, as recited in independent claim 13. Curry discloses a method, apparatus system, and firmware for secure transactions. According to Curry, a user module is capable of creating a random number and passing the random numbers with a request to a service providers equipment. The service provider e.g. may encrypt the random number with a private or public key

and pass the encrypted information back to the module as a signed certificate. The module decrypts and compares the random number received to the original random number (see col. 1, lines 48-67, of Curry).

The Examiner alleges that col. 7, lines 40-47, discloses the means for computing a first hash code in the payment machine. However, this section of Curry is part of a description of a digital Notary service. Modules are used as agents to provide this service (see col. 6, lines 63-66 of Curry). Each module is set up by the service provider to perform certification (col. 7, lines 1-35). An end user uses a hash algorithm to reduce a document to be certified to a 20 bytes message digest and the 20 byte message digest is sent to the input data object of the module (col. 7, lines 39-44). The transaction script of the module signs the resulting packet with a private key (col. 7, lines 43-47), and the end user stores the digital certificate. Since Curry discloses that the user performs the hash algorithm and that the module performs the certification, Curry fails to disclose a "payment machine comprises means for computing a first hash code from the material to be signed", as expressly recited in independent claim 13. Accordingly, independent claim 13 is also allowable over Curry.

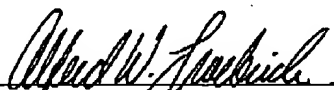
Dependent claims 2-12 and 14-17, each being dependent on one of independent claims 1 and 13, are allowable for the same reasons described above with respect to independent claims 1 and 13.

For all of the above reasons, the application is now deemed to be in condition for allowance and notice to that effect is solicited.

It is believed that no fees or charges are required at this time in connection with the present application. However, if any fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,

COHEN, PONTANI, LIEBERMAN & PAVANE

By 

Alfred W. Froebrich
Reg. No. 38,887
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: September 27, 2005